INCIDENTAL PAPER

Seminar on Intelligence, Command, and Control

Adapting the Military to the Homeland Defense and Homeland Security Missions
Dale W. Meyerrose

Guest Presentations, Spring 2003
A. Denis Clift, Dale W. Meyerrose, Roberta E. Lenczowski, John P. Stenbit, Patrick M. Hughes, James M. Simon, Jr., Richard Hale

May 2003

Program on Information Resources Policy

Center for Information Policy Research

Harvard University

The Program on Information Resources Policy is jointly sponsored by Harvard University and the Center for Information Policy Research.

E-mail: pirp@deas.harvard.edu URL: http://www.pirp.harvard.edu
ISBN 1-879716-86-0 **I-03-1**

May 2003

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University **Center for Information Policy Research**

Affiliates

AT&T Corp.
Australian Telecommunications Users Group
BellSouth Corp.
The Boeing Company
Booz Allen Hamilton
Center for Excellence in Education
Commission of the European Communities
Critical Path
CyraCom International
Ellacoya Networks, Inc.
Hanaro Telecom Corp. (Korea)
Hearst Newspapers
Hitachi Research Institute (Japan)
IBM Corp.
Korea Telecom
Lee Enterprises, Inc.
Lexis–Nexis
John and Mary R. Markle Foundation
Microsoft Corp.
MITRE Corp.
Motorola, Inc.
National Security Research, Inc.
NEC Corp. (Japan)
NEST–Boston
Nippon Telegraph & Telephone Corp (Japan)
PDS Consulting
PetaData Holdings, Ltd.
Samara Associates
Skadden, Arps, Slate, Meagher & Flom LLP
Strategy Assistance Services
TOR LLC
United States Government:
- Department of Commerce
  - National Telecommunications and Information Administration
- Department of Defense
  - National Defense University
- Department of Health and Human Services
  - National Library of Medicine
- Department of the Treasury
  - Office of the Comptroller of the Currency
- Federal Communications Commission
- National Security Agency
- United States Postal Service

Upoc
Verizon

Adapting the Military to the Homeland Defense and Homeland Security Missions

Dale W. Meyerrose

February 27, 2003

Major General Dale W. Meyerrose is the director of command, control, communications, and intelligence (C3I) at headquarters North American Aerospace Defense Command (NORAD), and the director of architectures and integration at headquarters U.S. Northern Command (NORTHCOM). He also serves as chief information officer for both commands. He ensures that the commander of NORAD has the command and control systems to safeguard the air sovereignty of North America. For NORTHCOM, he creates architectures and integrated solutions to support the command's mission to deter, prevent, and defeat threats to the United States. He also facilitates communications and information sharing for military assistance to civil authorities for crisis response and consequence management responsibilities assigned to the command. General Meyerrose entered the Air Force in 1975 and has spent most of his career in communications assignments, highlighted by service as a joint task force director of communications, as a joint communications support officer, and as commander of two major communications units. From 1994 to 1996 he served as the director of communications and information at headquarters U.S. Air Forces in Europe, and from 1996 to 2000 he was the director of communications and information, headquarters, Air Combat Command. Prior to assuming his current position, he served as director of command and control systems at headquarters, NORAD and U.S. Space Command, and director of communications and information, headquarters, Air Force Space Command. He wears the master communications badge and also is a master parachutist. He received a B.S. in economics from the U.S. Air Force Academy, is a distinguished graduate of the Squadron Officer School, received an M.B.A. degree from the University of Utah in 1978, and attended the National War College.

Oettinger: I take great pleasure in introducing to you General Dale Meyerrose. You've all seen his biography, so I don't need to go over that. I want to thank him for being willing to join us once again; he has been here before. Perhaps you have had a chance to look at his earlier remarks about cowpaths,[1] but his responsibilities have changed, and his topic has evolved along with

---

[1]Dale W. Meyerrose, "Networks, Information Technology, and Paved Cowpaths," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 2000* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-01-1, July 2001, [On-line]. URL:

them. So saying, I turn it over to you. I gather you are willing to be interrupted with questions, comments, and conversation.

Meyerrose: Thank you, sir. Not only can you interrupt me, but you can also change the topic if you want to. You can ask me any question, personal or professional, and I'm free to give whatever answer I think is appropriate. But I won't be offended. I also won't be offended if I drone on too long and somebody needs to go somewhere and meet another obligation. I totally understand. I will stay as long as necessary after the presentation and discuss with you any or all of the above, because I don't have an appointment until much later this evening. I hope we can have a good interchange.

I'm not going to go over any of my biography. Again, if there's something you want to ask about that, I consider myself free game while I'm in this non-attribution academic environment. If there is something that sounds pleasing or attributable, all you have to do is ask a question. I can let you do that, too.

The topic I'm going to start out with has to do with homeland defense and homeland security—a lot of the transformational organizational things that are going on within our government right now. It is an area fraught with a growing cottage industry of folks who are trying to jump on the bandwagon for political, economic, or ideological purposes. There are some precise definitions that our government is using in this area, and it behooves us, if we're going to spend any time at all on it, to understand what those are.

The first is that there is a difference in concept between homeland defense and homeland security, and that difference in concept also leads to a difference in who carries out those responsibilities and in what manner they do so. I'm going to start with homeland defense, primarily because everybody likes to start with the PowerPoint production picture that shows themselves in the middle, and that's the one where my command can be in the middle the longest.

If you were to look at a formal mission statement of my command, you would notice that it's a single sentence separated by a semicolon, with an equal number of words on either side of it.[2] The first phrase states a homeland defense mission, which has to do with deterring, preventing, detecting, and defeating military threats against the United States, its territories, allies, and possessions. It is a classic military mission. It is a mission that, if you changed the area of responsibility or the geography of the world, would be much like what you would find with other geographic unified combatant commanders—EUCOM [European Command], PACOM [Pacific Command], or CENTCOM [Central Command]. (If I say a word that's not familiar, please raise your hand, and don't be bashful, because there's probably some other person in the room who doesn't understand either.)

That is the centerpiece of homeland defense: a military mission. The Department of Defense [DOD] would be the lead federal agency; U.S. Northern Command would be the

---

http://www.pirp.harvard.edu/pubs_pdf/meyerro\meyerro-i01-1.pdf

[2]The command's mission is: "Conduct operations to deter, prevent, and defeat threats and aggression aimed at the United States, its territories, and interests within the assigned area of responsibility; and as directed by the President or Secretary or Defense, provide military assistance to civil authorities, including consequence management operations."

executing operational element. As you might imagine, there has been a lot of consternation about the name. It was specifically designed to contrast with U.S. Southern Command, which encompasses most (not all) of the Caribbean and Latin America down to Antarctica. NORTHCOM's area of responsibility [AOR] is a 500-mile boundary outside the coastlines of North America. In most people's view, that involves one, two, or three countries, but in fact the AOR covers eight countries: five in the Caribbean, and then Canada, Mexico, and the United States. There are a lot of political elements associated with that. Sometime during the question-and-answer time that I'm certainly going to leave at the end you may want to explore that. But it's a classic defense mission, with what you would consider the normal intelligence sharing, command and control processes, systems that support those command and control processes, et cetera. It is an environment that all of you who have a military background would be very comfortable in, because you would recognize it as being a military mission.

The second half of our mission responsibilities is what makes us truly different from the other nine unified combatant commanders. I probably should say eight, because my boss is dual-hatted as CINCNORAD and as the commander of U.S. Northern Command. There are nine unified combatant commanders, but ten unified combatant commands. Confusing? Sure.

The second part of that mission is what can be characterized as homeland security. Homeland security is not a defense mission, and in fact what you would consider homeland security within our U.S. government, by act of Congress and decree of the president, is the purview of the Department of Homeland Security. If you hear me use the abbreviation "DHS" that's what I mean.

Again, if you look at our mission statement, that homeland security piece has two critical elements. The first is that "Upon direction of the president and the secretary of defense…." We normally do not have a role in homeland security unless given that specific direction. Why? Because homeland security is the purview of another department, as of January 24 of this year.

The second thing that is critical about that part of our mission is that we will do it in support of a lead federal agency. Again, review: homeland defense equals DOD leads; homeland security equals some other federal agency that is not DOD leads. Most of you with military backgrounds are used to the terms "supported" and "supporting." "Supported" equates to who's in charge. "Supporting" equates to everybody responsible for either giving forces or resources or helping whoever's in charge accomplish some kind of a mission.

So there are two levels. When we support a lead federal agency, it will probably be in one of two types of missions. The mission will be consequence management, such as after a tornado, hurricane, or flood, or it will be crisis management, such as the East Coast sniper situation.[3] In most instances, when it is a crisis management situation the lead federal agency will likely be law enforcement-related, and for our purposes will in most cases be the FBI, the Federal Bureau of Investigation, or maybe, depending on the situation, a state government. If it is a consequence management type of situation—you all understand that consequence management means cleaning up some mess, restoring something to a new normal, if you will—then the lead federal agency in

[3]In October 2002, ten people in the greater Washington, D.C., area were killed and three wounded in a series of sniper attacks.

most instances will be FEMA, the Federal Emergency Management Agency, which is now being incorporated as part of the new DHS. A lot remains to be determined about how FEMA's processes will or will not change with the creation of Secretary's Ridge's organization.

If we provide forces or resources for either crisis management or consequence management, we come to the next level. We do so for two principal reasons. First, we possess a unique capability: one that no other entity within the United States possesses. Intercepting airplanes at 30,000 feet is one such capability. There is no other entity around, in any organization anywhere in our country, that is capable of intercepting airplanes at 30,000 feet. So if airplanes need to be intercepted at 30,000 feet, there's only one number you call.

The second reason for which we may be called upon to provide either crisis or consequence management support is when the capability is not unique to us, but the capacity of the owning agency becomes saturated. Two out of every three years, historically, in the western United States, we in the military provide firefighters or airborne platforms to fight forest fires. That capability does exist in several other agencies or services, or with contractors, but two out of every three years, on average, that capacity is exceeded by the need and so we provide support.

I've just given you the basic outline of homeland defense versus homeland security and the particulars by which we're carrying that out as the DOD in the executive part of the government. Notice that it took me longer to explain the homeland security part of the mission than it did to explain the homeland defense part of the mission, in part because I made some assumptions about your familiarity with military operations, and because, in terms of frequency, you almost never see us execute a homeland defense responsibility within the United States, but in fact we do execute homeland security responsibilities on a daily basis. We as American citizens do not want to see our military exercise its homeland defense mission. The reason is that it would be a means of last resort, and the consequences would be dire. There is nothing preventive, per se, when it comes to actually executing that mission, and of course "prevent and deter" is what we try to do at some point before we deal with military threats to our country.

Besides, when you're talking about support to another lead agency, whether it be a state agency or a regional agency such as CDC [Centers for Disease Control] or the American Red Cross, there are a lot of actors in there. One of the things that you realize in the course of creating a new command is that every early situation brings about a condition of discovery. Three weeks ago Saturday we woke up at 7:30 in the morning, and by 7:35 we had a whole host of new partners that we worked with because of the Shuttle disaster. In fact, we provided significant military forces. At one time there were up to 10,000 people somehow involved in the recovery and investigation aspects of the *Columbia* going down.

What we do in terms of homeland security is not new for the U.S. military, and there are instances throughout our 226-year history (I guess the Army would say it's 227; the country is 226, the Navy would say they're older than that). Doing those things, performing those functions, is not new. We've helped after floods, tornadoes, and other disasters, and there have been instances in which we've helped with restoring order under the Insurrection Act of 1795, the most recent example being the Los Angeles riots in April 1992. Another famous one that you may recall was in 1968, when Governor George Wallace attempted to block the attendance of black

students entering the University of Alabama. He activated the Alabama Guard to enforce that, which was in defiance of federal statute. We moved federal forces in to enforce federal law.

So the element of providing military forces for homeland security is not new. A lot of the processes—memoranda of understanding with organizations across the government—have been in existence for a long time, and many of those processes work very well. What has not worked well, and why we created NORTHCOM as a military entity, is a simple concept that those of you who are either in the military or looking forward to going into the military ought to understand very well. It's called unity of command. Unity of command provides you many things in terms of force employment and mission accomplishment. It defines the lines of command and control. It defines information sharing. It provides for a standing professional staff whose sole reason for existence is the continual planning, exercising, studying, certifying, and training of homeland defense/homeland security missions. In our short six-month history, it has provided us with a couple of other examples of what value added this command brings not only to the DOD, but also to the American people.

I'll use a couple of examples, which I know you're all familiar with. The sniper shooting incidents on the East Coast a few months ago were asymmetrical in their impact of terrorizing folks. People were afraid to go and pump gas at gas stations or to go into certain kinds of strip malls or roadside malls, because that's where some of the shootings had taken place. The law enforcement agencies came to the DOD and said, "We understand that you have unmanned aerial vehicles [UAVs], and we would like you to fly them over the East Coast to help us collect information to apprehend the individual or individuals involved." It sounds like a reasonable request, doesn't it? In fact, we turned them down for what they specifically asked for, because the effect they were hunting for had to do with providing an airborne platform from which to gather information or evidence, if you will, so they could prosecute. We were able to offer something else to them and say, "We have other airborne platforms, and we can stick a law enforcement—FBI—agent on the platform to gain custody of the chain of evidence. We can put an FBI official into the ground station so we maintain that chain of evidence." Ergo, we made a force provision tradeoff—one in which we understood what the intent was, we could look across the entire breadth of what the DOD set of assets and capabilities could offer, and we designed a capability to meet the situation that in fact protected the need-to-prosecute means of gathering information.

Student: Was that capability used, and used successfully, or was it irrelevant? Why is there a difference between having an FBI official in a large platform and having an unmanned platform overhead and having the FBI official at the ground station?

Meyerrose: Was it employed? The answer is yes. Was it employed successfully? The answer is yes. Was it employed effectively? I don't know, because it was employed within forty-eight hours of capturing the individuals and I am not privy to what information was gathered and whether or not it was used in the chain of evidence. That's the first part of your question.

The second part is a very interesting one that we deal with very often. You asked, "Why couldn't we just have one FBI agent down on the ground, and have a UAV up there?" I'll attack the flippant part of the answer first. There weren't any UAVs available, because we've got elements going all over the world. Second, the UAVs are not designed to use the satellite

telemetry over the United States; they're designed to use it somewhere else. So there were some practical employment problems—which we could have overcome, given a little bit of time.

However, the thing that is more important to look at instead has to do with the human in the loop and the business of chain of custody and things like that. Here is where we get into the elements where human processes, human thinking, human policies, human laws, and how we design to do things tend to lag behind what we can do technologically. What we did was follow the path of least resistance toward establishing a chain of custody that was least subject to argument, so that's why we did it. Again, it brings up an excellent question that we as a society have to struggle with all the time.

Let me give you another instance of where we made discriminating decisions, because we had the unity of command and had the full view of all the assets in the DOD to employ in a situation. The Shuttle *Columbia* went down. There were two separate phases with two separate lead federal agencies. There was the recovery phase, for which FEMA and the state governors of Texas and Louisiana were put in charge, and then there was the investigative part—again, the chain of custody of evidence that came through the atmosphere. They were two separate things, and NASA [National Aeronautics and Space Administration] and the FBI elements were the lead federal agencies. It wasn't the FBI for the purposes of law enforcement, but the FBI for the purposes of collecting evidence. Again, that changed very quickly, just as when situations escalate and become broader than we normally think they are.

Where do you think all these pieces fell, and what percentage of the Shuttle do you think actually survived burn-up coming through the atmosphere? What we were able to do was use a series of radars and observation elements, along with our scientists and physicists who made calculations, to help the NASA physicists and scientists pinpoint where things might be. Using GPS—Global Positioning System—equipment assigned to various folks out there helped to geolocate elements and speed up the element of recovering the remains of the Shuttle.

My point in all this is that for the first time in 226 years of existence our country has a single military person in charge of the defense of the homeland and responsible for whatever military forces are required to support homeland security. Never before in our history have we had a single military person empowered as my boss currently is.

Oettinger: As a practical matter, as a specified command is it mostly Air Force, or are there Army and Navy elements involved?

Meyerrose: Excellent question. In fact, it is not mostly Air Force. It is largely ground- and sea-based, and the two continental armies—First and Fifth—have the majority of the action. If you were to look at a cross-section of our staff, you would find it populated with about 28 percent Air Force, over a third Army, and then Navy and Coast Guard. In fact, the Coast Guard is an interesting element. If you look at the symbol of U.S. Northern Command you'll see five stars across the top, and they have to do with the five services from which we get forces. One of them is not a military service at all, but in fact is assigned to the Department of Transportation, and soon to be assigned to the DHS. It is called the Coast Guard.

Two days after we were created as a command, Hurricane Lily came across the Texas–Louisiana coast, so we fielded our first help call within two days. In my personal view the most valuable players we had in dealing with that first consequence management element were our Coast Guard officers (we only had about half a dozen of them assigned to our command), simply because they understood the environment better than we did as military officers, and they understood the constraints governing which of those processes were in play at what particular time.

That brings up an interesting point: how do you train and educate yourselves, since you are military folks, about hurricanes and weather? We find ourselves either visiting or conversing with elements or organizations that no other part of the military talks with. For instance, a month ago I made a West Coast swing. (I'm now going to tell you about my travels through sunny California, only it rained the whole time I was there.) I went down to San Diego, and my first appearance was talking to the Urban Institute of Search and Rescue. There was tremendous talent in a sector of society I had no idea existed. While I was in San Diego, I also met with their Port Authority. The next day I went up to Los Angeles, where I was hosted by the LAPD [Los Angeles Police Department], and I spent some time with the LA county sheriff, the LAPD, and the law enforcement jurisdictions in that part of the city, and again with port authorities. I went from there up to Oakland. You kind of get the picture that we have different partners. It's a different mix of people.

Oettinger: You singled out the weather as one of the elements of this. When I think back to World War II, weather intelligence and forecasting were critical for antisubmarine warfare and ultimately in the preparations for D-Day, et cetera. By and large, it was a military responsibility because there was nobody else to take it on and do it. Now you fast-forward to the current situation. What I hear you saying is that the evolution has every television station with its own satellites, and other private or government-owned satellite systems, and the military is essentially out of it. If I heard you right, you said there's no weather capability left in the military and it has devolved on someone else. Are there other areas like that, where there's been a massive shift in knowledge, know-how, and responsibility?

Meyerrose: First of all, if I gave the impression that the military has no weather capability that was a mistake on my part. In many respects, deep space weather and some of those things are very important to us in an economic, military, and societal way. Air Force Space Command in particular is deeply involved in that.

Most of the weather resources that we in the military have are aimed (if I can use that term rather loosely) at places where we historically have conducted military operations. We have not historically conducted military operations in the continental United States since Andrew Jackson defeated the British at the Battle of New Orleans. Of course, that was well before the National Weather Service was started by General A.J. Meyer, commander of the Signal Corps, in 1870. The National Weather Service, the Air Force, and a whole bunch of other folks started in the Army Signal Corps.

I may have given you the wrong impression, but let me pull that thread just a little bit more. Heretofore, we placed the elements of spaceborne platforms, and some of their functions, in space around the globe on the basis of where we were going to go in a military sense. A lot of that

capability is not over, nor does it service, North America, because we have not planned military operations in North America. So there are lots of things where the capability exists, but, because of how we've employed it over the past thirty or forty years, it does not necessarily support the missions that my command is responsible for.

Student: You talked about placement several times. I have some knowledge about space, and it seems that there's geosynchronous orbit, where you place something in a particular area, or polar orbit, where it hits everywhere.

Meyerrose: You have to be careful about saying it hits everywhere. It may have a track that creates a footprint on the earth, but that doesn't mean the function is geared to work in all parts of the orbit.

Student: Today's *New York Times* mentions that the Air Force has three observation facilities on the ground with high-power optical telescopes that can see very small things in orbit with very high resolution.[4] I had not heard of this before. It said a request had gone out from NASA to look at the STS-107 forty-eight hours prior to its coming down, and that NASA cancelled that request as being improperly worded. I was wondering if you could discuss that alleged capability. We know about the spy satellites that look down, but I hadn't known about the spy telescopes that look up.

Meyerrose: I'm going to paint a broad picture for you. I don't want to be too tutorial, but I think it bears a little bit of intellectual investment just to paint an accurate picture. In various places and locations around the globe, we have the ability to look into space for lots of reasons. In fact, we're the only country on earth that attempts to track every piece of what we call "space junk" or operational elements that currently orbit the globe. If you were to visit us in the Cheyenne Mountain Operations Complex, we could take you to the Space Tracking Center, in which that activity takes place.

The Space Tracking Center does use a series of sensors that include radar, telemetry, and other means of detection from various sources. Using those, plus algorithmic calculations, we determine where things are. That does not mean that we necessarily follow a piece of something orbiting in space twenty-four hours a day, seven days a week. There's no need to, because we have found out over the years that it would take way too many resources to do that. You've got 9,000 orbiting things up there as it is; 20,000-odd have already burned up in the atmosphere, or super-synched. What we do is take periodic readings of most of the things that orbit, and then, based on the calculations, do predictive analysis about where in fact they are.

One of the services that the DOD—specifically Air Force Space Command, Cheyenne Mountain Operations Complex, and NORAD—performs for NASA is to make calculations every time NASA launches from either Vandenberg or Canaveral in Florida to ensure there is an avoidance envelope around the thing that we intend to launch. It is possible to provide a focus on any piece of material, but what is not possible is to provide a focus on every piece all the time everywhere.

---

[4]"Loss of the Shuttle: Excerpts from NASA E-Mail about Space Shuttle Before It Disintegrated," *The New York Times*, 27 February 2003, A26.

That kind of describes the capability, and what I've just told you is that almost all the time our determination of where the 9,000-odd pieces are orbiting is based on a mathematical calculation, not on observation. That is theoretically good enough. Now, we can provide a stare, if you will. We can provide better stares at certain parts in space versus other parts in space just because of where the asset is. There are lots of requests that go from NASA to the DOD, which we fulfill on a routine basis, almost daily. I have no personal knowledge of the status of the request that you're talking about in the *New York Times* article—whether it was made, how it was made, or what the particular elements of it were. I'm sure that even if I did it would involve elements of the investigation part of the mishap and I would not be allowed to share them, but I don't know what they are.

Student: It was fairly widely publicized a week or so after the incident that the Air Force provided information to NASA. I think the news story may have been whether or not NASA made a request before re-entry, and what that request was, as opposed to the capability that you used.

Meyerrose: The capability does exist. It is the best in the world. It is widespread. It is global in nature, but it's not as global as everybody thinks.

Student: Getting back to the question of the mission, to what degree does your mission overlap with that of the National Guard and Reserves?

Meyerrose: That's an excellent question, because now we're getting down to some elements of constitutionality and what's legal in our country. That is very central to a lot of who we are and what we do. Again, many of you are better historians and better versed in American history than I am, but we all know that this country was founded upon a rebellion against centralized leadership, tyranny, monarchy, and all those things that represented control over the colonies that we didn't like. So, in the Constitution and in several of the statutes we put such things as "We may not employ federal troops against our population" and "We may not collect intelligence against U.S. citizens." We have some debate as to what a U.S. citizen is, and whether that extends to the person's computer in cyberspace or to illegal immigrants, et cetera.

A lot of the elements of what constitutes our militia and what it can do are embodied in what is called Article 32 of the U.S. Code. Article 32 outlines the broad parameters around which governors may use their militia within their state political boundaries, and those responsibilities are much broader than if we federalized the militia under Article 10 of the U.S. Code. Article 10 is what controls almost all of us on active duty—federal troops. The idea is that in the process of asking for help, a governor is supposed to look inward for resources to do something. For instance, if it's a law enforcement situation, one county sheriff goes to another county sheriff, or one law enforcement jurisdiction goes to another within the state. Traditionally, if governors choose to use their militia, they know that there are rules for what they can use them for. Can they give them guns? Can they pursue or apprehend? All those things are much broader than if you federalize them and make them federal troops.

The idea of first responders is an interesting thing that you need to delve into if you're interested in homeland security. First responders are the 100,000-odd police, firefighters, sheriffs, and so on who are out there. We train DOD capability to reside with the fifty states, four

territories, and the national capital region. We put it in the Guard, and use that as our linkage to what governors do. We do it fairly often.

The first easy example is what we call a DCO—a defense coordinating officer—who is assigned to either the First or the Fifth Army, assigned with the Guard in a particular state. When something happens, that individual becomes the advisor to the governor or the on-scene FEMA commander or on-scene FBI commander as to what capability—if they need it and if they ask—they can get from the military.

Another easy example of collocating a capability with the Guard forces is what we call CSTs—crisis support teams. These are small teams with small command and control packages. They are the first folks on scene to provide initial capability for other folks who would be called in later should the decision be made to expand the scope of the activity. The linkage between the Guard and the Reserves is one that will only grow in terms of process and identification and practicing with my command in the future.

The question that I've avoided for the past ten minutes or so is one of relationships. I've talked about homeland defense being the purview of U.S. Northern Command. I'm going to expand the question beyond the original intent. The question was: "I thought NORAD was in charge of aerospace defense, so what's the fracture line here?" First of all, there is no fracture line, because the commander of both organizations is the same. By the way, I have a role in both organizations: I'm the J-6 [director of command, control, communications, and intelligence] of both. Neither General Eberhart nor I sits there and says, "Okay, I'm doing *this* with my NORAD hat on, and *this* with my NORTHCOM hat on." It's an element of performing the mission, regardless of what hat you wear, and if there's paper to follow it sorts itself out.

NORAD provides the forces for air sovereignty over most of the North American continent. It is a bilateral command between us and Canada, and forever we've ignored the fact that Mexico is part of North America. There are a lot of historic reasons behind that, and clearly that's something that we need to work toward and factor into the future. But NORAD still has aerospace defense responsibilities for North America. NORAD still has regions and sectors that control fighters on alert at various locations, and are designed to respond to not only the threat of somebody flying in from the outside trying to do us harm, but also somebody launching and flying from the inside. Again, that's one of those site picture changes that 9/11 brought us. So, in that regard, NORAD is a supporting command to NORTHCOM, which has the responsibility for the defense of America, Canada, and everything within 500 nautical miles of the coastline of North America.

Oettinger: NORAD is a strictly aerospace command, as opposed to NORTHCOM, which, as you explained before, has multiservice representation.

Meyerrose: That's correct. Eighty percent of those whom we would call NORAD officers come from an air-type organization, versus the other kinds of organizations.

Student: I was going to expand it to the command and control, and I think you're alluding to it heavily here. You have the aerospace mission, which is traditionally under NORAD. NORAD owns those assets. With NORTHCOM, it seems there are a lot of assets that aren't necessarily

owned by NORTHCOM. In that case, at certain times would NORTHCOM become like a combatant command that just borrows assets? How does that command and control and peacetime coordination occur?

Meyerrose: That's an excellent point. It comes about just as it does with almost every other geographic combatant command. If I used the terms COCOM [combatant command], OPCON [operational control], ADCON [administrative control], and TACON [tactical control], do you know what I mean? If you aspire to move into the military you need to understand what those are. COCOM is like command of assignment: it's the highest level of ownership. It's where everybody's efficiency reports come from, as well as their money and their unit of assignment and everything. It's the broadest, most encompassing relationship a headquarters can have with subordinate organizations. In fact, we only have about 1,000 people who are COCOMed forces. I'm a COCOMed individual to U.S. Northern Command, just as I am to NORAD.

OPCON means that you temporarily have control over forces. Let me give you an example using another command. CENTCOM's General Franks only owns about 2,000 folks who occupy his headquarters. All of the forces that are in Southwest Asia are OPCONed to him. He does not own them. His components—his air, maritime, and land component commanders, or force providers—have given him forces to command in combat, but he does not own them. He does not have to equip them, modernize them, train them, or any of those kinds of things, which are largely service responsibilities. How many B-2s does CENTCOM own? The answer is zero. All nineteen B-2s are at Whiteman Air Force Base, Missouri, but there's not a geographic commander anywhere in the world who can't get B-2s assigned to do missions for him. All he needs is an execute order, and a force provider, namely Air Combat Command, provides them.

By the same token, we are for certain situations given OPCON over forces, by which we direct them to do something. Let's go back to our aerospace defense mission. Most of that, if you're at all familiar with it from the U.S. perspective, is flown by Guard and Reserve F-16 and F-15 pilots. While they're sitting there in their squadrons at their home locations they come under Article 32 of Title 10 of the U.S. Code, or if they're a Reserve force it's Article 5. We in the DOD don't necessarily fund them, train them, provide their mandate, or do any of those other kinds of things. As soon as we put X number of aircraft on alert, they become OPCONed to NORAD. If they respond against an external threat in our forward area, then NORAD is the supported command. If they are employed against an internal threat—inside that AOR—they become a supporting command to NORTHCOM. It's all made simpler because General Ed Eberhart is the commander of both.

Oettinger: Let me make a sidebar here, because General Meyerrose's presentation today has been centered on relations between the military and the civilian, which have come to the fore by virtue of the homeland security issue. In these last three minutes, he has encapsulated fifty years of very complicated history of the relationships among different elements of the military. Within a couple of weeks you'll be reading Allard's book, which goes into considerable detail about the history of the arrangements that he has just talked about.[5] It also talks about the genesis of the

[5]C. Kenneth Allard, *Command, Control, and the Common Defense* (New Haven, Conn.: Yale University Press, 1990).

Goldwater–Nichols Act of 1986, which took the notion that disparate services, which were kind of okay in Revolutionary times, weren't exactly the most satisfactory way of doing things in the 1980s and 1990s, and addresses how the structure of the military was changed for greater coherence by the Goldwater–Nichols Act. Aside from its historical value in understanding the military, you also ought to read that book in terms of what it may tell you about the problems arising in this relationship between the military and the civilian sides.

What triggered this was the mention of OPCON and so on. There are a couple of books by a retired Army general named Jack Cushman on command and control that were also instrumental in the passage of the Goldwater–Nichols Act and go into great detail about the pre-Goldwater–Nichols flaws that were meant to be redressed.[6] For example, a commander who had OPCON over certain forces could not court-martial somebody who was not performing properly. It had to go back to the service. Little details like that make a great difference in terms of perception, operational efficiency, et cetera. So when you get to Allard keep in mind what you heard in the last three minutes, and put it into the context of the military–civilian issues that are prospective. You may get some guidance for your papers on that.

Meyerrose: You made some excellent points. Let me give you the Meyerrose version of many years of bureaucratic, organizational roles and missions. We talked about warfighters. It's fashionable to talk about warfighters, and all the people who consider themselves operational entities within any of our services consider themselves warfighters. They cannot be warfighters unless they are assigned to one of ten unified combatant commands. Only then can an airman in the Air Force, or a sailor in the Navy, or a soldier in the Army, or a Marine in the Marine Corps, actually become a warfighter. The services are here to "organize, train, and equip," and of course it's very fashionable for us in our services to say, as we do in the Air Force, for instance, "Our mission is to fly and fight, and don't you forget it." In fact, the Air Force does not fight. Airmen who are operationally controlled by unified combatant commanders can indeed become warfighters, but while they're in the Air Force they technically cannot. It's the same with the Navy, Marine Corps, and Army. So one group is force employers, the other is force providers. It's kind of a good way to think of it. Again, I'm probably making some assumptions. I don't know that I understand all this either.

Student: I understand you're the J-6 for both NORTHCOM and NORAD. For NORTHCOM you're the director of architecture and integration, and for NORAD you're the director of command and control systems. Why the difference? Why are they both J-6? Are they the same, but just with different names? I'm kind of interested in that.

Meyerrose: So am I. One I inherited, the other I picked. How's that for an answer? The one I inherited was with NORAD, which is why I said earlier, kind of flippantly, that there are still four CINCs in the U.S. military. We had a decree that said there's only one CINC in the United States, and that's the president. He is the only one who can be commander in chief. But we've got three exceptions. Those three exceptions are because they are called out in a treaty to which the United

---

[6]John H. Cushman, *Role of the Major Operational Commands in the Evolution of Command and Control Systems* (Bedford, Mass.: The MITRE Corporation, 1980); *Command and Control of Theater Forces: Adequacy* (Washington, D.C.: AFCEA International Press, 1985).

States is a signatory, and we made a conscious decision that we're not going to redo the treaty just to change the name. You've already got one: CINCNORAD. Does anybody know who the other two are? SACEUR [Supreme Allied Commander, Europe], and CINCUNK [CINC, U.N. Forces, Korea], because those are titles used in the treaty. I'm sure that when the treaty is rewritten the title will be changed. That's just a little bit of trivia that means absolutely nothing to anybody.

Back to my flippant answer of "one I made up and the other I inherited." The one I inherited was the NORAD one, which is deeply rooted in how NORAD did business. We have not changed our NORAD titles, simply because that structure is predicated on a lot of things that had unintended consequences. If you think of the J-6 as being somebody who makes sure that systems work and commanders can exercise command and control and those kinds of things, that's what I do on both sides of the house.

The reason why we elected to give me a different title under NORTHCOM has to do with being "transformational." You can relate back to our transformation discussion at lunch a little bit if you like, but we had come to the understanding that we needed an element that is more of a horizontal integrator, and one that spans a broader part of the mission than the historical technical systems support. That's what is connoted by the title of "architectures and integration." I am the command architect for operational architectures. I have mostly operators putting operational architectures together, because I do it for the operators. I don't put all the techies in there. I work systems architecture, for which I end up with a mix of techies and operators and planners. Then, when I get to the technical architectures, that's obviously dominated by the more technical folks. The title has the connotation of a broader level of responsibility. Also, integration of processes, information, and things like that across the command is not necessarily tied to systems, but has a broader, more important human element to it. So what you see is the first step in making the J-6 more than just a techie advisor on the staff and more of a cross-command operator, planner, and implementer. Fundamentally, I have the same responsibilities for both commands; hence, I'm the J-6 for both.

By the way, we're the second newest command, by two hours, in the U.S. military. The newest command is STRATCOM [Strategic Command], which was born two hours after we were, even though they're one hour earlier in the time zone, but that's beside the point.

We struggle with what we call the Napoleonic structure of J-codes based upon functionality, versus some sort of "transformational" organization based upon effects-based capabilities. In the short term, my commander has elected to straddle both, in that we justified our manpower on the basis of the Napoleonic J-structure, but when we employ forces to any large degree we matrix ourselves into four primary groups: the operational planning group, the current operations group, the joint planning group, and the information superiority group [ISG]. The whole staff matrixes itself into those four governing bodies that then run the processes of worrying about effects-based capability. I happen to head up the ISG. In there you will find the information operations people, the public affairs [PA] people, the networks people, and the intelligence people—a lot of those skills that make up that group. We work how each of those skills contributes to information superiority.

Similarly, the joint planning group is headed by our J-5, whom most of you would recognize in the Napoleonic structure as being the senior planner of the organization. In fact, all

of the Js contribute skills of certain types to that joint planning group, and they end up worrying about the effects-based results and capabilities and consequences of future activities, actions, force posturings, allocations, entitlements, and all those other kinds of things. We have the COG, the current operations group, which, as you might imagine, worries about the close fight, and then the operations planning group worries about the mid-range fight that chronologically follows the close fight. Those, as you might imagine, are dominated by operations folks, but in fact all of us have skills that are part of those groups.

Student: Could I ask you a little more about how that ISG is working out? That sounds a lot like some of the ideas in the Navy and the Marine Corps. People are talking about having a knowledge manager, but as an intelligence type, which is my background, I'm worried. Maybe it's just because it means that I'm not going to be in charge anymore, but how is it working to combine those fields under one hat, which happens to be yours?

Meyerrose: First of all, you shouldn't think of my hat as being the J-6. I am one of four two-stars on the staff. Theoretically, we could have given me one of the other groups and put the J-3 [director of operations] in charge of the ISG. One could make the case that that's the proper thing to do, because in my kind of command, situation awareness and handling information may be fundamentally different from the force employment business of other commands. We chose not to do that, but one could make that case. Instead of looking at me as the J-6 in charge of the ISG, you need to look at me as one of four two-stars on the staff, who's in charge of one of the four capabilities- or effects-based set of elements.

Is it working? The answer is: I don't know. It's a very new stand-up. We've gone through one exercise with it. If you want some information about this, it is really patterned after the Millennium Challenge structure that came out of the Joint Forces Command exercises of last year. It would behoove you to look at that, because it forms the intellectual foundation on which we formed the group.

Let me give you my personal style on how you go about forming an organization and not threatening everybody. Again, I may use some traditional terms, but we're trying to figure out what others to use. We're not even sure that "information superiority," even though that will be the joint standard, is the proper title for use by U.S. Northern Command. Information superiority and the use of force within the United States connote a dominance that maybe we don't want to connote in a military organization. There is some baggage that goes along with them that has to do with intelligence gathering and things like that, which we are not in favor of within our country against our citizens. Information superiority associated with anything having to do with our own citizens bothers us, doesn't it? So maybe I need to change the name of the ISG. I don't know.

Oettinger: This is the first time I've heard a semi-coherent explanation of effects-based outcomes. I was expecting something like "zero hijackings over the United States," and out comes something like information superiority. Why do we have an Air Force whose effect is information superiority when the issue is to avoid hijacked airplanes plowing into tall buildings? Can we step back a bit and explore why you're going down that road? I understand the Napoleonic headings—you've got to have intelligence, you've got to have folks who do

something, you've got to have folks who plan—but I'm not understanding those four groupings at all.

Meyerrose: Again, this is the natural friction point, if you will, between functionally aligning and orienting a staff versus mission alignment.

Oettinger: Yes, but the missions don't make sense to me.

Meyerrose: What you've got is a process by which you handle missions. Those groups are not missions in and of themselves, but the charter for how they operate has to do with coming up with a different functional grouping than "The intelligence assessment is *this*; the ops recommendation is *that*; the planners' recommendation is *this*; the communications support recommendation is *that*."

In my position as head of the ISG, the things I worry about—and again, I'm going to use the military terms that we are challenging—are "What's the red view of blue?" What is the enemy's view of friendly forces? In a homeland defense element, it's pretty easy to say, "What's Al Qaeda's view of the United States?" But are we as Americans comfortable with calling Americans "blue forces"? Of course not. We have to develop a language that takes those paradigms and adjusts them into something that's acceptable and palatable. What is Hurricane Lily's view of the southeastern coast of the United States as it approaches three days out?

Student: It's a target.

Meyerrose: You bet! Now, do you think Americans like being considered targets? Of course not. So, again, we're struggling with the business of taking military paradigms and terms, because they have processes with which we're familiar, and trying to morph them into a situation in which they fit into homeland security and homeland defense.

Again, as I approach the element as the head of the ISG, I never once tell the PA person how to do his or her job in the context of working with the Associated Press, United Press International, news stations, or whatever. However, the PA people feed into an information dissemination plan that we develop as a command, for which I'm responsible. They provide many of the skills and perform many of the actions that I do not supervise per se, other than to say that they are meeting the commander's intent for a marketing plan or a communications plan or an information dissemination plan. I don't stand up as a hierarchical briefer and say, "The PA guy told me to tell you this." It's the same thing with intelligence. I don't interfere with any of the intelligence people if they have the skills to do their job. I'm responsible for making sure we establish where they fit in and what their linkages are to the commander's desired effects overall.

Student: Would you say, sir, that you're essentially sort of a coordinator rather than a commander in a military sense?

Meyerrose: We only have one commander in my command.

Student: So what you're saying is that you're not the direct boss in the reporting chain, for instance.

Meyerrose: No. However, the J-2 [director of intelligence], who is in the direct reporting chain, is a part of my group, so the business of reaching down to the JOC [joint operations center] or JAC [joint analysis center] or JIC [joint intelligence center] or whatever we call them these days is related to my job in some ways. See what I mean? Again, these are learning processes. We try not to trip over the names, but we first try to implement the concept and then back into the label that most appropriately describes the concept. Of course, we have to fit our JACs into the element of "The president said he was going to institute a national intelligence gathering agency oriented toward homeland security and homeland defense." We still need to work those processes out. What do we give them, and what do they give us so we don't needlessly duplicate, but instead back each other up and meet each other's needs in terms of information sharing?

Again, how well is it working? The answer is that we're in the infancy stages. Here's the thing that was hard to get across, and is still hard to get across to some of the folks in our command: we're not talking about J-2 guys coordinating better with J-3 guys coordinating better with J-4 guys, coordinating better with the JIC. It's not a level of coordination we're talking about. We're talking about feeding effects-based outcomes. It's a different way of thinking.

Student: What is the hardest problem you're facing now, aside from the confusion over structure and aside from the policy questions of gathering intelligence on U.S. citizens? Taking all that off the table, what's the hardest thing in terms of your getting your job done? Is it training your forces? Is it budget? Is it the unavailability of high tech? What's in your way?

Meyerrose: Again, the low maturity level of processes is probably the biggest hindrance. "Gathering intelligence on U.S. citizens" is not a problem for me, and you don't have to take it off the table. It's not on the table to start with. If that's going to take place, that's somebody else's problem. That's not my job.

It is the element of maturing the process of how you interact. It is very easy for us to make calls to FEMA, or field offices, because we've established who everybody is. But how do we provide the horizontal sharing of information among all the participants in, say, an incident at the Hoover Dam? How do we create that trusted information exchange environment, separate from the one that has to do with civil unrest in Dade County, Florida? Simultaneously, how do we keep that information exchange environment separate from (I have to be careful what I say here) some kind of incident in a port on the East Coast. And, if they end up being related, how do we then create the new environment that cross-flows information across organizations or departments?

Student: From what you're saying, it sounds as though your primary concerns are structural: bureaucratic constructs. What I don't hear from you is that there are specific capabilities or technologies that you feel you're at a loss for.

Meyerrose: That's because I don't feel I'm at a loss for technical capability.

Oettinger: It seems you're committing an error by characterizing these problems as "bureaucratic." It's not logic chopping over the lines of command. It has to do with very fundamental issues of constitutionality and effectiveness. If you go back to the earlier example about the FBI guy in the airplane, maintaining the purity of evidence as it passes from one hand to another is an essential element of law enforcement. An intelligence person doesn't give a

damn. It gets in the way. So you're talking about actual performance of a mission and, by virtue of the difference between police and military or, as we like to think of it, between civilian and military, you're talking about Constitutional issues. They manifest themselves in all sorts of bureaucratic overtones, but if you look at them as though they were merely bureaucratic hassling you'd be missing the point. We are recalibrating the whole structure of relationships between different elements of the government and the governed. If you don't have the consent of the governed in our society you have serious problems. They have bureaucratic overtones, but they're rooted in fundamental Constitutional and reformist criteria. Is that a fair assessment?

Meyerrose: That is eloquently said, and it's not my job to challenge the legal framework. It is my job to figure out how to make the statutes that we have work: how to complete missions in accordance with the national will, federal statutes, state statutes, and the like, because they are fundamental underpinnings of our society. That is why, in the homeland security element, we will always be a supporting, subordinate element, not a supported, controlling element.

Oettinger: The good news is that he's doing exactly what a serving military officer should: obeying the law and obeying commands as they are given. Your role in this classroom, whoever you are and whatever you may do outside the classroom, is to look at all of that and ask "Does it make sense? Did it make sense yesterday, does it make sense today, and how could it be tomorrow?" The Constitution and the laws aren't God-given; they're evolving, and some of this may need reinterpreting. If you guys aren't prepared to think about it, nobody else will.

Meyerrose: Those are excellent points. If I can revisit the earlier question, I want to give you something else to think about. In the business of NORAD, NORTHCOM, air, and all that kind of good stuff, how about missile defense? That is something that we're politically struggling with, not only within our own government, but also with our neighbor to the north, Canada. So you need to think through that. What parameters do we currently have in aerospace defense that are applicable to missile defense? Which ones are not covered, and so what policies do we need to establish in order to cover them? You may know that we're in the middle of providing studies about, "Is a missile launched from North Korea aimed at North America the responsibility of PACOM, STRATCOM, NORAD, or NORTHCOM?" In terms of the supported/supporting that we talked about with NORAD and NORTHCOM, there is no answer yet. We have studies that are making recommendations, and think tanks, military organizations, and organizations contracted by each government are also doing that. You need to crank that kind of thinking into your scope of trying to figure this out.

Student: This goes back to the four groups that you've aligned yourselves into, and I'm not sure I have those groups right. It sounds as though there are two ops groups—current and longer-term ops—and a planning group and an information superiority group. If I have those four right in my mind, I'm trying to think about applying those four mission-based groups to missions like missile defense or aerospace defense, and how they align themselves against those missions more properly than maybe the J-code setup does. I'm not sure I see there's necessarily an advantage. Maybe there's an example of where it gives you an advantage that the traditional organization didn't have.

Meyerrose: I don't know that I can give you a situation, because you talked about those missions in terms of "who's responsible for missile defense?" That is a strategic-level question, and you need to boil down your scope to an operational-level analysis of what we do and why we do it and how we do it. We end up with execute orders, or we have operations plans or communications plans or all kinds of mechanisms that cause us to plan for, anticipate, move, enforce, or do whatever we do. In essence, what we do is take a structure with a cross-staff or a cross-population set of expertise to focus on phases of employment or reaction. The only one that's not necessarily focused on phases would be the ISG. The ISG would be going all the time, because it's a situation awareness mission that supports the other three groups and then changes during execution time, whereas the ops groups and the planning group are oriented toward campaign accomplishment.

What percentage of the time does the staff stay in the Napoleonic, Joint Staff configuration, and what percentage of the time does the staff spend in the operational, mission-executing portion? We don't have the answer to that, but some of our senior mentors in some of our exercises seem to imply that we need to have a mission-oriented staff up and running twenty-four by forever. As long as there are terrorist threats or incidents and all those kinds of things affecting this AOR, there is a constant campaign for which you need to be mission based. Like most organizations, we go from 100 percent J-code and 0 percent executing the campaign to 100 percent executing the campaign and 0 percent J-code. It's that hot/cold, on/off kind of thing that we are currently battling. We say, "You know, you ought to be organized and trained the way you would fight a campaign, or a war." That ends up being this effects-based kind of structure.

Oettinger: For those of you who want to pursue that sort of thing, unless I misunderstand you, the literature on matrix organizations and the tug of war between the skills and the missions is a place to look. There is no "one size fits all" answer.

Meyerrose: In fact, if you look at corporate America, that is a constant theme in a lot of major corporations. What kind of overarching company organizations do you allow to exist outside of product centers? The product centers would closely correlate to the four groups we have, and overarching corporate headquarters organizations would equate to the J-directorates. Again, while the particular elements of each don't necessarily translate, the overall discussion about the cost tradeoff between company-wide governance organizations as compared to product center entities is very applicable.

Student: In terms of executing your current new missions in NORTHCOM, how much do pre-existing structures or even physical systems within NORAD force you to "pave cowpaths," as you put it in your previous talk?[7]

Meyerrose: In reality, very little. The closest analogy to paving a cowpath from NORAD has to do with the air picture, or common operational picture on the air side, that we provide. The other elements are not very closely related. NORAD didn't track what high-interest vessels are in port, or where storms are hitting the North American coast. NORAD does have some role in Space Shuttle launches and paths of clearance and things like that, but it's not much. It's mostly based

[7]See note 1.

on command and control, and a sense of technology, and in fact does not permeate across the board in our processes within NORTHCOM.

Student: I'm curious about the J-2, or the intelligence side of the house in your organization. It's unlike other combatant commands out there. What do the intelligence officers in your command—I assume you have some permanent ones in the organization—do? Are they within the Defense Intelligence Agency? Are there new duties going along with these interactions?

Meyerrose: They drink coffee…

Student: Now wait! They're not allowed to drink coffee on duty!

Meyerrose: I'll probably be a little awkward in describing this, because I'm trying to break it down into basic stuff. First of all, the overall construct for our intelligence community is not necessarily set up like a military organization. In fact, the intelligence community will tell you that it extends outside the DOD. For reasons of creating centers of excellence, there are definite places where we go to in our intelligence community for specific kinds of low-density, high-demand kinds of expertise. For instance, not every intelligence officer can interpret a space photo image. We have small centers dispersed around the government that have those technical skills, apply them, and share the results in a distributed fashion to all intelligence-supporting organizations.

We will probably maintain a few analysts associated with airborne things, because we still have a NORAD mission, and then we will either import, tap into, or grow analysts who support homeland security and homeland defense. There will be a tradeoff in terms of how many analysts will be in the DHS, the FBI, and all those other places. It is the responsibility of the intelligence community to reach out to the most appropriate place for that capability, because we don't raise, grow, field, equip, or man every single command to perform all of its intelligence functions. Right now, we're carving out a niche, if you will, within the intelligence community regarding what expertise or centers of excellence we will grow in my command, which will contribute to the intelligence community in a larger sense for use not only by the DOD, but also by other folks who have access to that information.

Oettinger: You have just hit on another element that one might inadvertently characterize as bureaucratic, but it has its roots in money. Everybody ideally would like to have every kind of expertise as an organic component under their own control, but nobody can afford that. Ergo, you have to go to the situation that General Meyerrose describes, where you have certain centers that do this, that, and the other thing. Ergo, there will be what looks like a bureaucratic fight over who's working on what for whom when, and are you going to do my work or somebody else's work, and what are your priorities? That's another whole area that you've opened up for serious consideration, and you might want to save some of your questions along those lines for General Hughes and for Jim Simon when they come.[8] They'll be able to spend their whole time here addressing the kind of question that you've raised.

---

[8]Patrick M. Hughes and James M. Simon addressed the seminar on March 20, 2003, and April 10, 2003, respectively.

Meyerrose: They would be perfect individuals to answer that question.

Student: Where does force protection fall into your mission?

Meyerrose: Excellent question! By the way, when we go to orange from yellow, what does that mean? I don't know. What we're discovering is that if you don't have good entrance and exit criteria it hard to get yourself out of the infinite do-loop. This was a lesson that we in the military learned in spades in Vietnam. So guess what? When it came time for Desert Storm, the military worked very hard on what the exit criteria were. When do you declare success, and when do you get out? Obviously, a lot of that is rooted in political questions, and then how do you link military action to that political decision?

Force protection for us is a fundamentally different thing than force protection for, say, the commander of EUCOM. The reason is that in excess of 90 percent, or virtually all, of the forces in the EUCOM AOR are COCOMed by the commander of EUCOM. That means that he's the one who determines when they go to Force Protection Alpha or Bravo or Charlie. In this AOR, as I say, we have 1,000, so .001 percent of the forces in this AOR are COCOMed to us. By the way, you end up with the same discussion when you talk about computer network operations and STRATCOM, because in fact STRATCOM does not COCOM the networks of the DOD, but they're owned and operated by virtually every command.

So, strictly speaking, the elements of force protection that we have to do with affect only the 1,000 people who work for us. However, we do have a larger responsibility in advising the secretary of defense, his staff, the Joint Staff, et cetera—a lot of that advice based upon the intelligence that we gather and are informed about—and making recommendations for certain force protection activities and actions. That's a preventive mechanism. When there is a crisis, and it is a homeland security force protection issue, if directed by the president or the secretary of defense we provide force modules for somebody else to use to control the situation. If it is a homeland defense issue—last resort, dire consequences—then you'll probably see another, stricter, more urgent type of direction coming out.

Our ability to make force protection determinations for forces in our AOR affects every other AOR, because this is the deployment, force employment, and training base. If we locked everybody in the United States down in Protection Level Delta, that all of a sudden would cut off the mobilization pipeline to CENTCOM, EUCOM, PACOM, or some other kind of operation that's not in our purview. By the way, are there corollary actions when we go from yellow to orange to red, and how does that relate to the five-tier FEMA grading, and how does that relate to the four-tier FBI grading, and how does that relate to…? Just pick an organization, and they've all got their own pet rocks in how they name them.

At the last unified combatant commanders' conference in January, General Eberhart brought up that very point, and the secretary of defense took an action and tasked that to the Joint Staff to work. It says, "We've a whole mix of things here that we need to examine in detail, figure out what makes sense, and then make a proposal from the DOD to the government at large that makes it a lot easier for there to be relationships and corollary actions so that we don't confuse ourselves and the American people as to what the real situation is." Again, that's a work in progress. It's something we've got to grow into, and we're not ignoring it. How fast we're going to get the

whole government to agree on the same numbering system is up in the air. I think we ought to go to the Dewey Decimal System. All you have to argue about is which number is higher or lower, but the numbering system is established, so you just pick your number.

Student: If you come down from the macro to the micro level, earlier on you described a series of incidents across the country that at first glance don't necessarily seem to be interrelated, but gradually, as information comes in, may prove to be linked in some way. On the technology side, are there new technologies for information sharing between agencies and the first responders whom you don't classically think of as DOD or related to national security, but under the new homeland security umbrella are going to have to share fairly high-level classified information? What's going on there in terms of the technology? What new strategies have been developed?

Meyerrose: That, again, has to do with our desire to create a shared environment for trusted information exchange. You said something about classified information. First of all, we in the DOD are the only ones who generate classified information—TOP SECRET and so forth. No other place do you find that. It may be proprietary, or peculiar to an organization, and they may treat it like classified information, but the only classified information within the context you're alluding to is DOD-related.

A bunch of the information you're talking about does not originate in the DOD domain or transit a lot of the DOD domain, but still must interface with it. For instance, let's say that a first responder, such as a Coast Guard cutter, intercepts a high-interest vessel that supposedly has ship-jumpers on it, or has known hazardous cargo, or arms, or whatever. I'm sure you realize that some of those scenarios are played out. Then there's geolocation. How do you establish the geolocation? Is the geolocation established because you've been monitoring the ship via certain technical systems, or is the geolocation established because the first responder is on the scene and the uniform or the helmet that individual is wearing has a GPS radiating chip that gives the geolocation? Is the geolocation classified? There are all kinds of elements.

I would tell you there's not a single technology issue in all this. If you're in the information technology business, Web-linked technology, object-oriented networking, and all those kinds of things, while they're not ancient, have been around for some time.

I will leave the city unspecified. I had the county sheriff on one side, and another law enforcement agency on the other. I noticed they had a certain kind of radio, but the sheriff had a different model than the other guy. I was familiar with the radios, so I said, "What frequencies do you transmit on? Do you have the chip that allows you to program independently?" "No, we don't." "Okay, why don't you spend $19.95 and get the chip in your radio so that you can communicate on his frequency and you can exchange information?" The reaction was, "Why would I want to do that?"

Oettinger: You can also look at New York City. The arguments between the fire department and the police department are on record, and the solution to that is still far from being achieved.

Meyerrose: There it's not a chip in the radio, because they all have radios that will interoperate, provided they allow them to. So the technology is there. Do we have the process or the mindset or

whatever to implement it to overcome the lack of horizontal integration or flow of information? That's the harder question, and it's not one that I'm sure we're going to solve.

Oettinger: If you want to read a little more about that, in our seminar proceedings there's a fellow named Kawika Daguio, who was the American Banking Association's representative on the President's Commission on Critical Infrastructure Protection.[9] You'll see that the sensitivity of information in the banking industry, while not legally classified, is almost equal. That will give you another example of the private sector sensitivities to the use of various kinds of information. It is totally policy- and politics-oriented in terms of what sector of our society has what kinds of needs and concerns over information that it holds.

Student: Could you address your group's role in the protection or defense of critical infrastructure?

Meyerrose: We haven't settled on the definition of critical infrastructure either, and that's a governmental issue. I don't know if you realize it or not, but the government came up with several lists of prioritized critical infrastructure, and there was a lot of political dissension, because some folks thought they were important enough to be on the list and weren't. All politics are local.

Student: Everyone is essential personnel on a snow day.

Meyerrose: Exactly! So determining what is critical is, again, not our responsibility per se. However, having said that, there are some general guidelines about what critical infrastructure things we will assist with on a routine basis. When cities host large events, such as the State of the Union address in Washington, D.C., or the Super Bowl in San Diego, we continue to fly routine combat air patrols [CAPs] randomly around the country, on the basis of what is happening, what threats we perceive or think may materialize, as a show of force, and as a means of pre-positioning assets with which to engage some sort of attack. We do that on a daily basis. It is random, and where we do it becomes known after the fact.

Student: Is that strictly post-9/11?

Meyerrose: We have been positioning air defense assets around the North American continent since 1957 and the start of NORAD. The way we do it today, and the randomness and the frequency and the numbers involved, are post-9/11.

Student: Last summer, the president issued the National Homeland Security Strategy, and one of the mission areas within that was critical infrastructure protection. That mission area was assigned to the DOD, specifically to Northern Command within the United States, just as the other mission areas were assigned to different departments, such as Commerce or Transportation.

---

[9]Kawika Daguio, "Protecting the Financial and Payment System by Dispelling Myths," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 1999* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-00-2, June 2000, [On-line]. URL: http://www.pirp.harvard.edu/pubs_pdf/daguio\daguio-i00-2.pdf

As a matter of fact, there are twelve areas, each assigned to a different part of the government. The only one was assigned to the DOD was critical infrastructure protection.

Student: More specifically on that, could you address how the capabilities developed during the cold war are being upgraded or are continuing their use in today's environment?

Meyerrose: We're working at making the sensor structure and grid, which we had looking outward during the cold war, look inward as well. There's an example of something we started in the cold war, we've completely reoriented it, and we're in the process of upgrading it. We're in the process of upgrading many of the technical command support structures that were originally fielded in the cold war and we're continuing, such as the command and control structures in NORAD, STRATCOM, and those kinds of things.

There are a lot of things that we're shedding from the cold war. The element of forward basing is an obvious one. I don't know how many troops we have stationed overseas on a permanent basis. Look at the massive troop reductions we've made in Europe and the Pacific! At its zenith in the late 1970s, we had close to half a million troops in Europe, and now we're down to around 100,000. So a lot of our force postures and policies from the cold war have been changed. Any tool that we manage to keep or decide to keep gets transformed, if you will, into a new mission.

Student: I meant more what you were touching on before about critical infrastructures.

Meyerrose: We're continually refining what we think we mean by "critical infrastructure," and that will largely be a political determination. Our response to it will be a military determination, but the definition, the policy, and who's going to be accountable for it will largely rest with the policymakers.

Student: Maybe I'm beating a dead horse here, but I'm sure you've established a linkage and a relationship to some degree between NORTHCOM's response to defending critical infrastructures and the homeland security threat level changing from orange to yellow or whatever. You're really responding to the threat at the most appropriate level, but if the threat is somehow reflected in the changing color scheme, do you have a critical infrastructure response that matches the different levels on the homeland security scale?

Meyerrose: At a broad, theoretical level, yes. In fact, when the country went to orange, most of the military facilities went to Bravo in terms of changing force protection conditions and reactions and posture.

Student: And your CAPs that you might be flying as a defensive measure would be based on whatever threat caused you to go to that level, right? They wouldn't necessarily just be preprogrammed responses associated with that level. The response would be appropriate to the threat.

Meyerrose: That's right. I will cite specifically something that was reported in the news. As many of you may have read, the news claims that we have put air defense artillery units in and

around the Capitol. In that fabric is a correlation and relationship of what we do in response to what the larger security posture is.

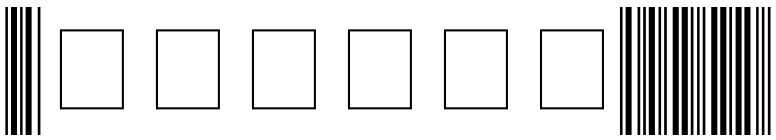
Oettinger: This is going great guns, but we are approaching the witching hour, so I would like, on behalf of all of us, to thank you very much and give you a token of our appreciation.

Meyerrose: Thank you very much. I wish you all good luck. This is an exciting time in the history of our country. I'm sure that every time thinks it's an exciting time and it dwarfs all others.

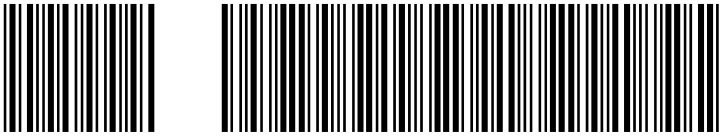
I'll leave you with one parting thought, primarily because many of you are officers in the military, and some of you aspire to be officers in the military. The oath of office that we take, and that many government officials take, has a long history in our country. The phrase that starts it off has been in existence since 1868. It says, "I will support and defend the Constitution of the United States against all enemies, foreign and domestic." I know that in 1971, when I first took that oath, and in 1975, when I took it as a commissioned officer, "support and defend the Constitution of the United States against all enemies, foreign *and domestic*," didn't quite have the meaning that it has for me post-9/11/01. Again, that is an obligation that maybe has a slightly different impact on all of our lives, and it's very reflective of the times we live in. I wish you all the best of luck in your endeavors and your studies. Take advantage of every opportunity you have to live and grow and enjoy life and contribute what you can.

Acronyms

AOR	area of responsibility
C3I	command, control, communications, and intelligence
CAP	combat air patrol
CENTCOM	U.S. Central Command
CINC	commander in chief
COCOM	combatant command
DHS	Department of Homeland Security
DOD	Department of Defense
EUCOM	U.S. European Command
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
GPS	Global Positioning System
ISG	Information Superiority Group
JAC	joint analysis center
JIC	joint intelligence center
JOC	joint operations center
LAPD	Los Angeles Police Department
NASA	National Aeronautics and Space Administration
NORAD	North American Aerospace Defense Command
NORTHCOM	U.S. Northern Command
OPCON	operational control
PA	public affairs
PACOM	U.S. Pacific Command
STRATCOM	U.S. Strategic Command
UAV	unmanned aerial vehicle



Seminar2003



ISBN 1-879716-86-0